Tinexta Cyber Risk Report 2024

Malware, Phishing e Ransomware

tinexta cyber

www.tinextacyber.com

Chi siamo

Tinexta Cyber

Parte del **gruppo Tinexta**, nasce dalla sintesi di tre eccellenze – **Corvallis, Swascan** e **Yoroi** – con l'obiettivo di supportare le organizzazioni nel raggiungimento dei propri traguardi, favorendo una crescita sostenibile e promuovendo resilienza e sicurezza.

Tinexta Cyber unisce l'eccellenza nella protezione digitale ad un approccio innovativo alla system integration.

Un punto di riferimento per le aziende che cercano soluzioni avanzate e sicure, grazie a tecnologie proprietarie e competenze all'avanguardia.

Un polo in grado di creare ambienti digitali robusti, performanti e modulari; dove sicurezza e tecnologia si uniscono per garantire un futuro digitale sicuro e senza compromessi.

Tinexta

Tinexta è un Gruppo industriale che offre soluzioni integrate per la **trasformazione digitale** e la crescita di PMI, grandi gruppi e istituzioni. Quotata all'Euronext STAR Milan con un solido azionista istituzionale di riferimento, è inserita nell'indice europeo Tech Leader come azienda tech ad alto tasso di crescita.

Nata in Italia e presente in 12 Paesi tra Europa e America Latina con oltre 3000 dipendenti, Tinexta è attiva nei settori strategici del **Digital Trust, Cybersecurity, Business Innovation.** Attraverso le società del Gruppo, si posiziona come partner strategico di riferimento nel campo dell'innovazione digitale, offrendo servizi avanzati per l'identità e la certificazione digitale, la cybersecurity, le tecnologie per la sicurezza nazionale e lo sviluppo d'impresa.

SOMMARIO

Disclaimer

La ricerca svolta da **Tinexta Cyber** è basata su dati OSINT e CLOSINT ottenuti tramite l'utilizzo di tecnologie proprietarie di Threat Intelligence. Questa pubblicazione non rappresenta necessariamente lo stato dell'arte – data la natura transitoria delle fonti – e **Tinexta Cyber** si riserva la prerogativa di aggiornamento periodico. Fonti di terze parti sono citate a seconda dei casi. **Tinexta Cyber** non è responsabile del contenuto delle fonti esterne, compresi i siti web esterni a cui si fa riferimento in questa pubblicazione. La presente pubblicazione ha uno scopo puramente informativo. Essa deve essere accessibile gratuitamente. Né **Tinexta Cyber** né alcuna persona che agisca per suo conto è responsabile dell'uso che potrebbe essere fatto delle informazioni contenute in questa pubblicazione.

Data collection Notice

Il presente rapporto è stato redatto esclusivamente dai professionisti di **Tinexta Cyber,** mediante l'utilizzo di tecniche di Open Source Intelligence (OSINT) e Closed Source Intelligence (CLOSINT), oltre alle piattaforme e tecnologie proprietarie di **Tinexta Cyber**. Le informazioni raccolte e presentate in questo documento rappresentano solo la parte emersa dell'intera situazione, poiché sono state prese in considerazione esclusivamente le aziende colpite da attacchi di ransomware che, avendo rifiutato di pagare il riscatto, hanno subito la pubblicazione dei propri dati su siti di data leak.

Si sottolinea che il numero riportato nel presente rapporto riflette un trend generale basato sulle informazioni disponibili. Tuttavia, è fondamentale comprendere che tale dato rappresenta solamente la punta dell'iceberg, in quanto il numero reale di vittime potrebbe essere significativamente superiore, considerando un fattore moltiplicativo n volte più grande.

Tinexta Cyber non può garantire l'esattezza o la completezza delle informazioni fornite nel rapporto, poiché tali dati sono soggetti a cambiamenti e possono essere influenzati da vari fattori esterni. Gli utenti sono pertanto invitati a considerare attentamente il contesto e la complessità della situazione prima di trarre conclusioni definitive o prendere decisioni basate su queste informazioni. Si declina ogni responsabilità per eventuali conseguenze derivanti dall'uso delle informazioni contenute nel presente rapporto.

Tinexta Cyber si impegna a mantenere la massima riservatezza e professionalità nelle proprie attività di analisi e fornisce questo rapporto a scopo informativo senza assumersi alcuna responsabilità legale o di altro genere.

Obiettivi del report

Il **Tinexta Cyber** Risk Report si propone di offrire un'analisi approfondita e rigorosa delle principali minacce informatiche emerse durante il corso **del 2024,** concentrandosi su quattro aree cardine: Common Vulnerabilities and Exposures (CVE), Malware, Phishing e Ransomware.

Il report mira innanzitutto a monitorare e analizzare le minacce emergenti, fungendo da guida per comprendere l'evoluzione del panorama delle minacce informatiche globali. Attraverso un'accurata raccolta e analisi di dati OSINT e CLOSINT, il nostro intento è delineare le tendenze principali in tema di attacchi, identificando le vulnerabilità critiche e i settori più esposti, in modo da fornire alle organizzazioni le informazioni necessarie per implementare adeguate contromisure.

In un contesto in continua evoluzione, è fondamentale tenere traccia delle tecniche di attacco sempre più sofisticate adottate dai cybercriminali. Il report esplora come ransomware e phishing abbiano continuato a mutare, diventando più mirati, e fornisce una panoramica delle strategie emergenti, come la combinazione di attacchi multi-stage e l'utilizzo di tecniche di evasione avanzate.

Un obiettivo centrale di questo documento è anche quello di fornire alle organizzazioni raccomandazioni strategiche per mitigare i rischi derivanti da queste minacce. Analizzando le vulnerabilità più rilevanti, si invitano le aziende a implementare protocolli di sicurezza basati su tecnologie all'avanguardia e approcci proattivi.

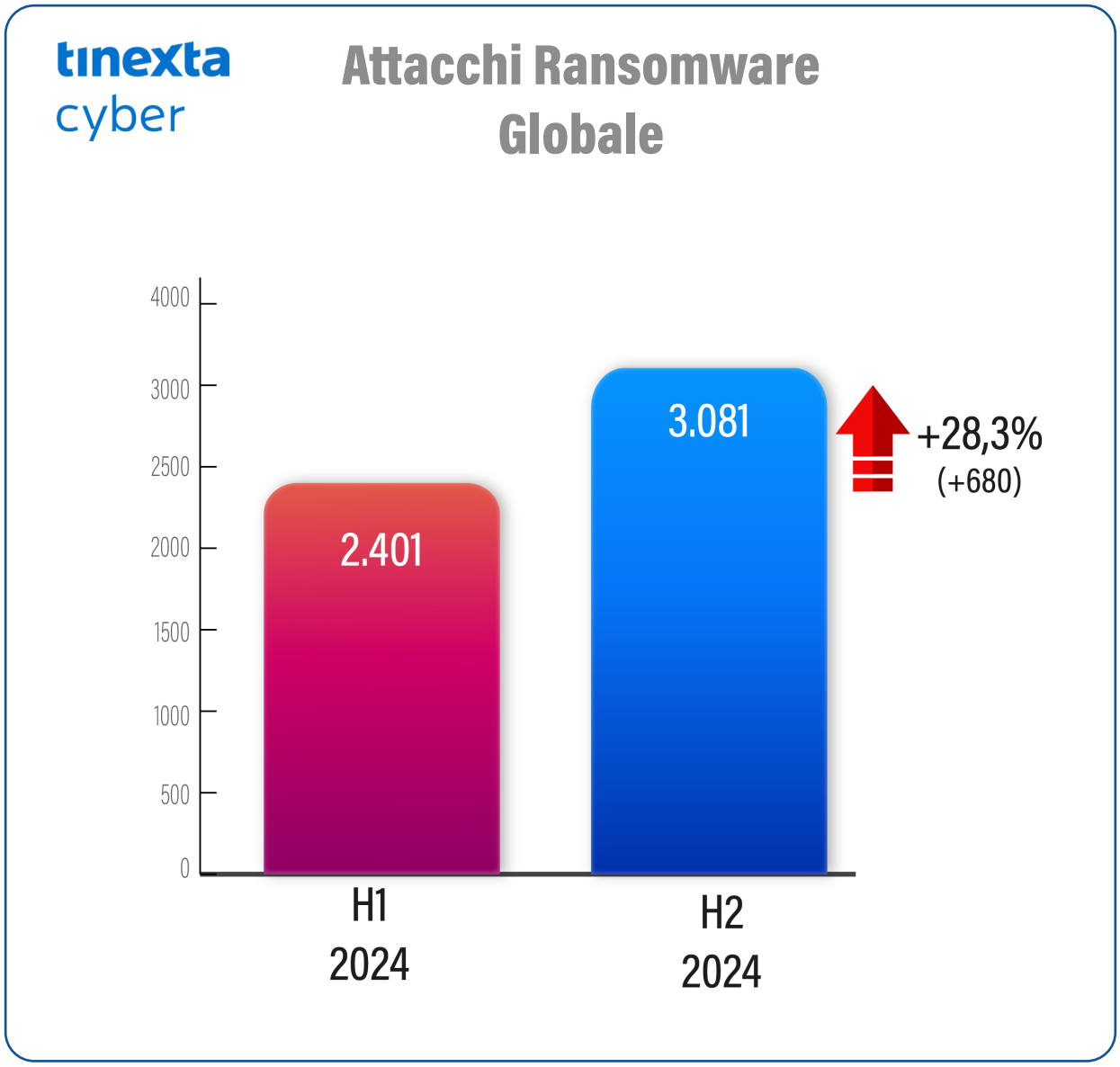
In aggiunta, il report intende accrescere la consapevolezza e la cultura della sicurezza informatica tra i leader aziendali e i responsabili della sicurezza. Promuovere la necessità di adottare una visione olistica della cybersecurity, che combini prevenzione, monitoraggio continuo e capacità di risposta agli incidenti, è cruciale in un contesto di minacce in costante crescita. La consapevolezza del ruolo centrale che la sicurezza informatica ricopre nella salvaguardia della continuità operativa e della reputazione aziendale è di fondamentale importanza.

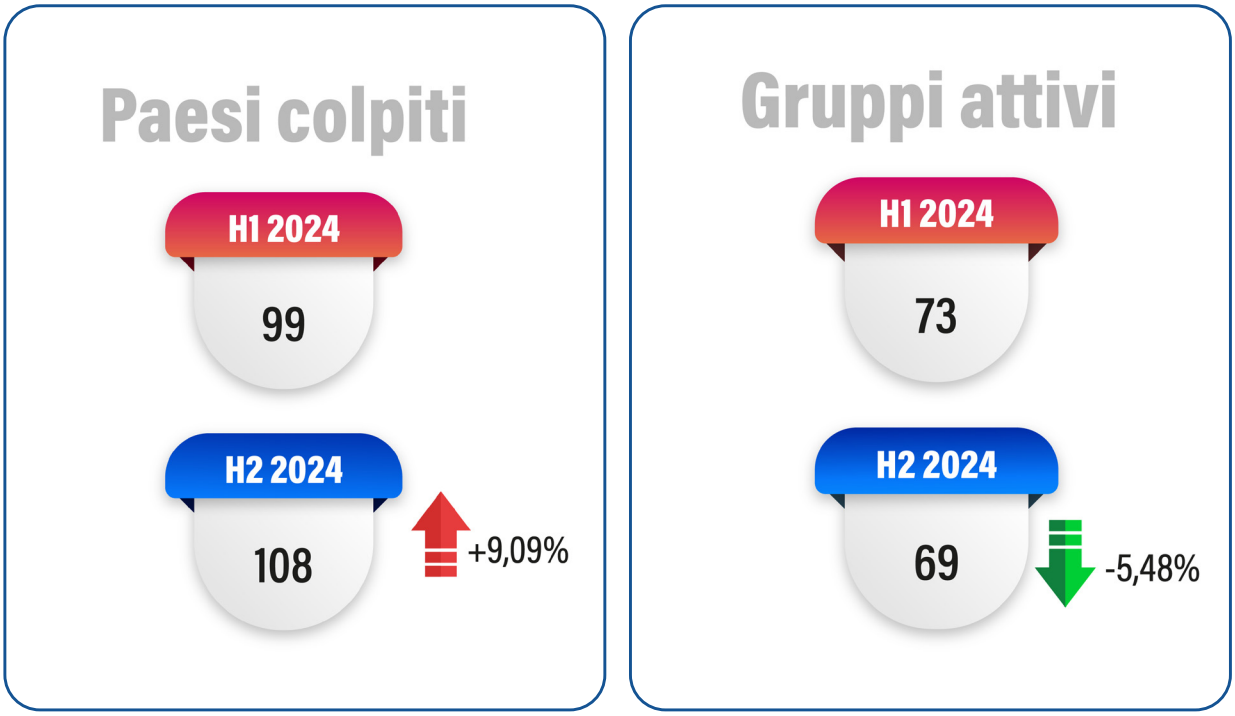
Questo documento offre una visione strategica per supportare la resilienza delle organizzazioni contro le minacce emergenti, evidenziando l'importanza di un approccio integrato alla sicurezza. Questo non deve limitarsi alla protezione delle vulnerabilità tecniche, ma deve includere anche la salvaguardia dell'intera catena del valore, compresi fornitori e partner strategici.

Un primo sguardo

Nel passaggio dal primo al **secondo semestre del 2024**, si osserva un significativo incremento delle vittime e dei paesi colpiti da attacchi ransomware, mentre il numero di gang attive ha mostrato una leggera diminuzione.

Le **vittime globali** sono **aumentate del 28,30%**, e i **paesi colpiti** sono **aumentati del 9,09%**. Tuttavia, **le gang attive** sono **diminuite del 5,48%**.





Tra i **paesi più colpit**i, gli **Stati Uniti** continuano a registrare il maggior numero di vittime, con un aumento del 32,70%, seguiti dal **Canada** (+19,70%) e dal **Regno Unito**, che ha visto una diminuzione del 18,62%. Un nuovo ingresso nella top 4 è **l'India**, che con una percentuale di vittime significativa si afferma tra i paesi più colpiti. Per quanto riguarda **l'Italia**, le vittime sono **aumentate del 6,67%**.

A livello delle gang, alcune delle più consolidate, come **LockBit** e **Medusa**, hanno ridotto significativamente la loro attività, mentre nuove gang come **RansomHub**, **Argonauts** e **Sarcoma** hanno ampliato le loro operazioni.

In **Italia**, in particolare, è stato osservato un aumento delle minacce, con un **incremento del 14,29%** rispetto al semestre precedente, e un crescente coinvolgimento di gang come RansomHub e DragonForce, che hanno intensificato la loro attività.

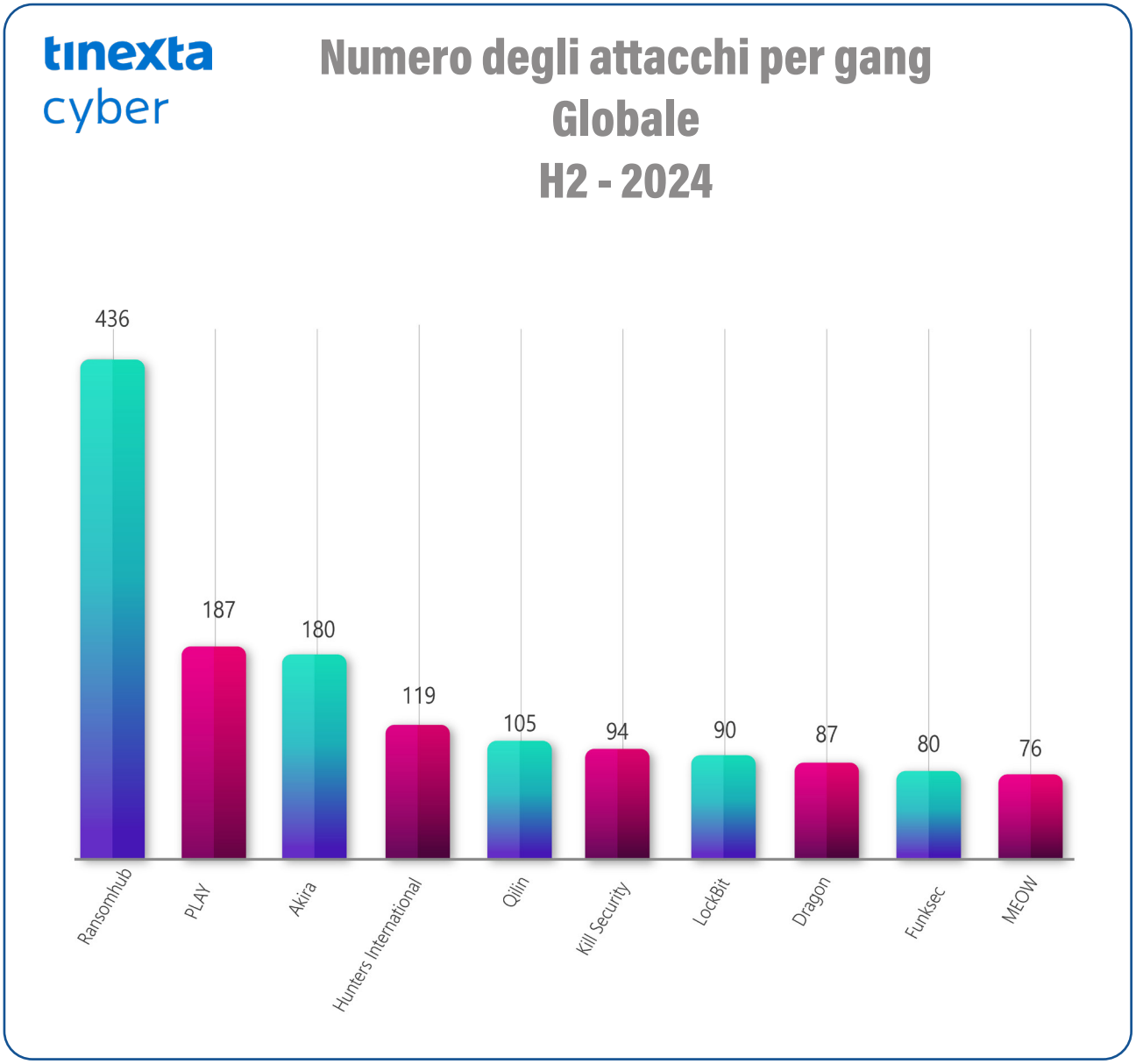
Il settore **manifatturiero** ha visto il maggior incremento di attacchi, passando dal 20% al 32%, mentre il settore dei **servizi** ha registrato una riduzione significativa (dal 18% all'8%).

Le aziende più colpite sono state quelle con un fatturato tra i 0 e i 250 milioni di dollari, sebbene vi sia stato un leggero calo rispetto al semestre precedente.

Anche i **malware** hanno mostrato una notevole evoluzione nel secondo semestre del 2024, caratterizzatisi da una maggiore sofisticazione nelle tecniche di infiltrazione e di sfruttamento di vulnerabilità.

A fianco dell'aumento degli attacchi mirati al settore manifatturiero, è emerso un uso sempre più strategico da parte dei cybercriminali di piattaforme legittime (GitHub, Google Ads, Zoom Docs) per diffondere malware come Lumma Stealer e AMOS, che sfruttano la fiducia degli utenti in servizi legittimi.

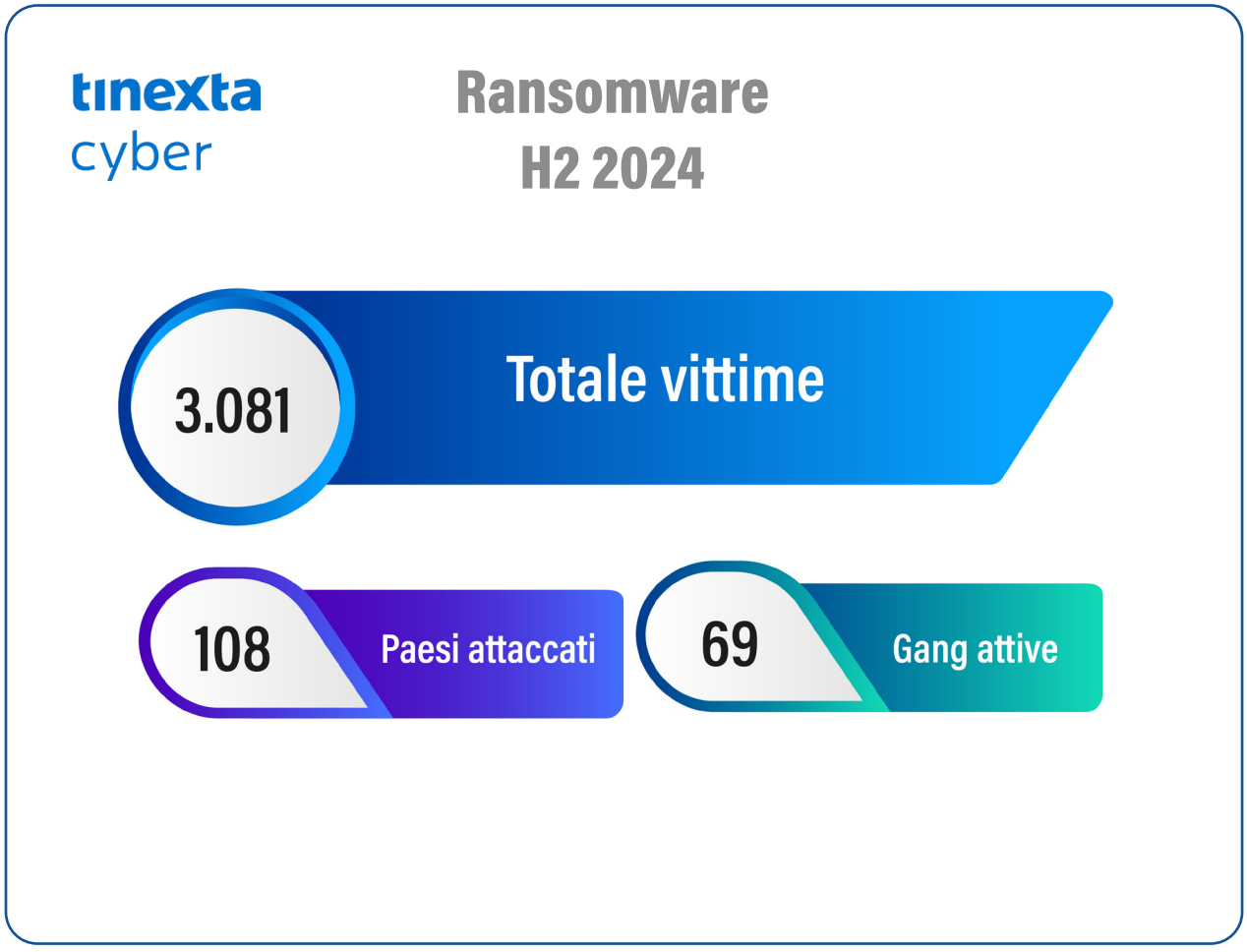
L'integrazione dell'IA nelle campagne di **phishing** ha reso gli attacchi più realistici e difficoltosi da individuare, con e-mail e messaggi personalizzati che simulano accuratezza il linguaggio di istituzioni e aziende. In parallelo, il settore delle criptovalute è stato bersaglio di strategie come l'address poisoning e i falsi airdrop, sfruttando l'interesse crescente per queste tecnologie. Nonostante la riduzione del numero di gang attive, la diffusione del modello Malware-as-a-Service (MaaS) ha reso accessibili anche a operatori meno specializzati strumenti avanzati come FormBook e AgentTesla , amplificando la minaccia per aziende e utenti finali.



Ransomware

Il 2024 si è caratterizzato per una escalation senza precedenti negli attacchi ransomware, con dinamiche che hanno ridefinito il panorama della cybersecurity a livello globale.

Nel passaggio dal primo al secondo semestre, il numero di vittime è aumentato del 28,30% (**da 2.401 a 3.081 casi**), mentre i paesi coinvolti sono cresciuti del 9,09% (**da 99 a 108**). Questo trend, apparentemente contraddittorio con la riduzione del 5,48% delle gang attive (**da 73 a 69**), suggerisce una concentrazione del potere criminale in mano a gruppi più organizzati, capaci di sferrare attacchi su larga scala con risorse ottimizzate.



La diminuzione delle gang potrebbe riflettere anche l'efficacia di operazioni internazionali di contrasto, come sanzioni mirate o arresti di figure chiave, che hanno indebolito gruppi storici come **LockBit** (−43,06%) e **Medusa** (−99,17%).

Tuttavia, questa contrazione ha lasciato spazio a nuovi attori, come **RansomHub** (+25%) e le new entry **Argonauts** e **Sarcoma**, che hanno sfruttato il vuoto lasciato dai predecessori per espandere la propria influenza. Questi gruppi emergenti hanno adottato strategie più aggressive, combinando attacchi multi-vettore e tecniche di evasione avanzate, come l'exploit di vulnerabilità zero-day o il ricorso a infrastrutture decentralizzate per evitare il tracciamento.

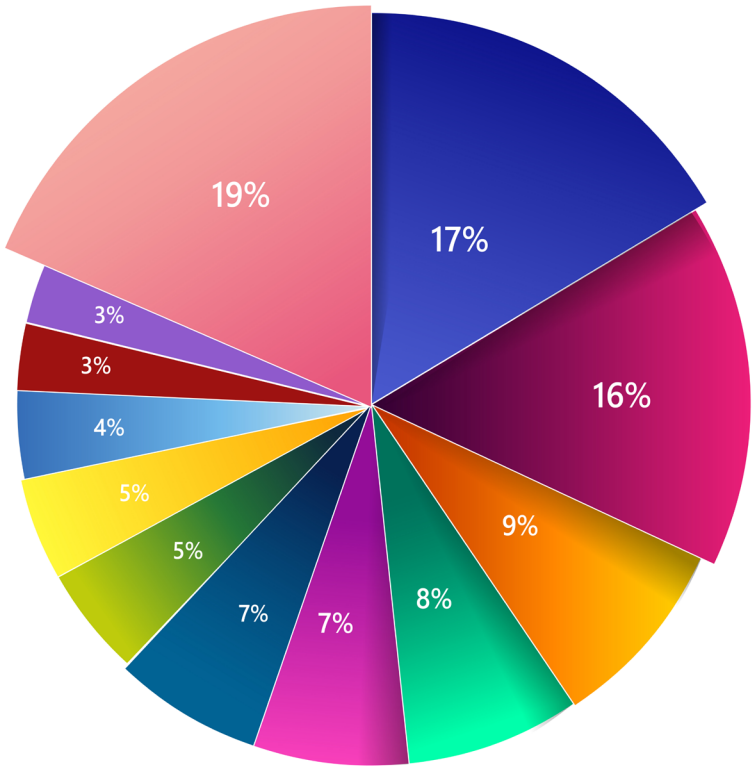
A livello geografico, gli **Stati Uniti** hanno consolidato il loro ruolo di principale bersaglio, con un aumento del 32,70% delle vittime (da 1.176 a 1.561), seguiti da **Canada** (+19,70%) e India, che ha fatto il suo ingresso tra i paesi più colpiti con 90 vittime. Il **Regno Unito**, invece, ha registrato un calo del 18,62% (da 145 a 118 vittime), probabilmente grazie a investimenti mirati in difesa cibernetica e collaborazione pubblico-privata. L'**India**, nuova nella top 5, riflette la crescente digitalizzazione del suo tessuto economico e la vulnerabilità di settori come la sanità e i servizi finanziari, spesso non adeguatamente protetti.

Top 8 paesi colpiti (H2- 2024)

Settori e obiettivi: una transizione verso l'industria pesante

tinexta cyber

Attacchi per settore (Globale) H2 - 2024



tinexta
cyber

Top 4 settori colpiti H2 2024

Manufacturing: 17%

Le fabbriche utilizzano macchinari connessi a Internet (IoT industriale) e spesso sistemi SCADA, che possono essere meno aggiornati dal punto di vista della sicurezza. Inoltre, i tempi di inattività in produzione sono estremamente costosi, il che spinge le aziende a pagare rapidamente il riscatto per ripristinare le operazioni, rendendo così un obiettivo remunerativo. Molte aziende manifatturiere non investono abbastanza in sicurezza informatica rispetto ad altri settori.

Services: 16%

Settori come il turismo, l'ospitalità e il commercio al dettaglio gestiscono molte informazioni personali e finanziarie dei clienti, rendendoli un obiettivo per i criminali informatici. La continua operatività dei software gestionali e dei sistemi di pagamento è fondamentale. Un attacco ransomware può bloccare le operazioni e spingere le aziende a pagare il riscatto.

Construction: 9%

Le aziende edili collaborano con più fornitori, subappaltatori e partner, aumentando le superfici di attacco. Questo settore spesso non dispone di infrastrutture informatiche avanzate, né di politiche di cybersecurity ben definite.

Finance: 8%

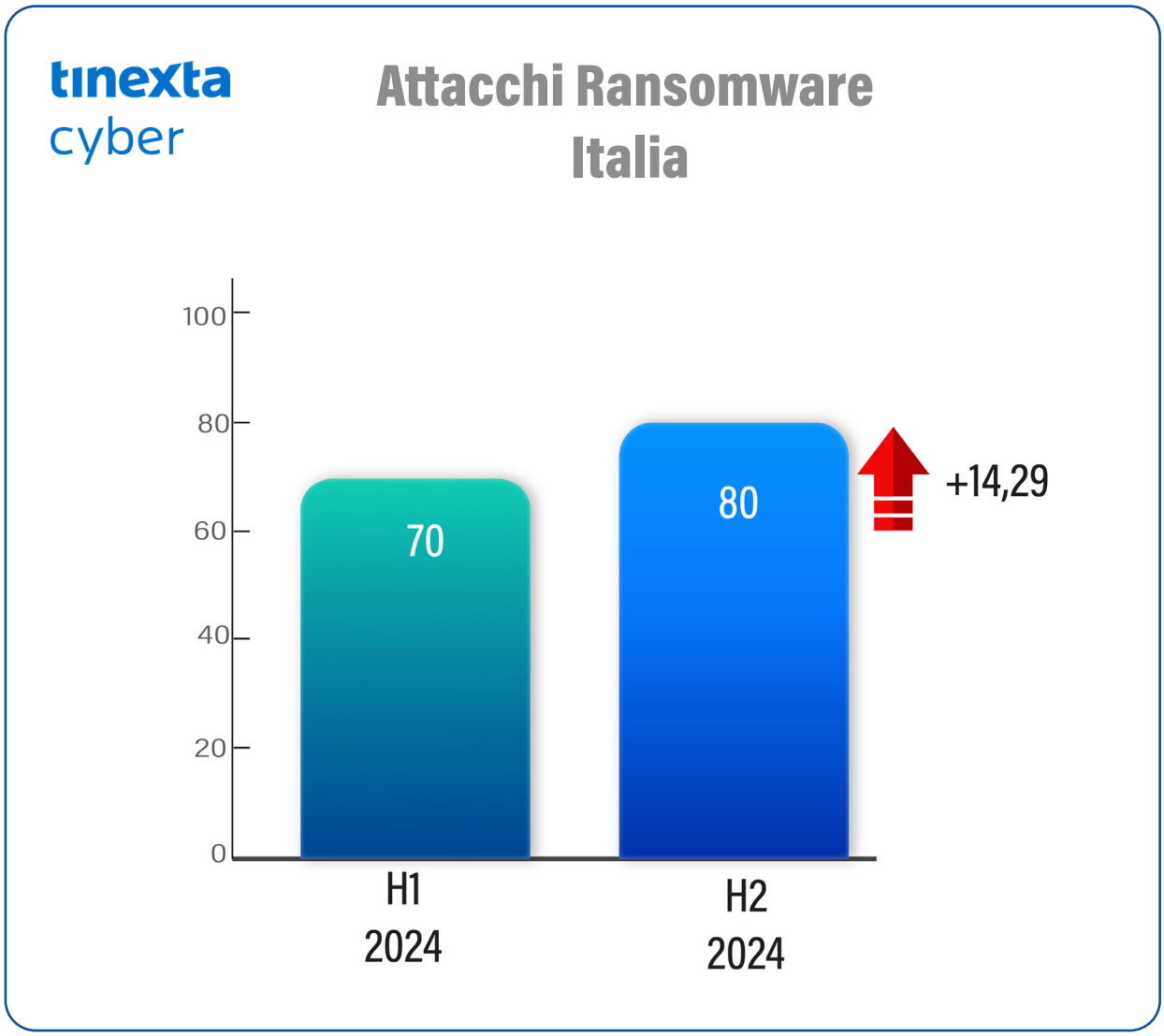
Le banche e le istituzioni finanziarie custodiscono enormi quantità di dati sensibili, come informazioni bancarie e personali, molto redditizie per i cybercriminali. Inoltre, il rischio di sanzioni per una violazione dei regolamenti riguardanti la privacy dei dati è elevato, il che può portare le aziende a pagare il riscatto per evitare multe e danni alla reputazione. Gli hacker sviluppano ransomware più avanzati per eludere i sistemi di sicurezza delle banche, spesso con l'obiettivo di esfiltrare dati prima della crittografia.

In generale, questi settori sono presi di mira principalmente perché:

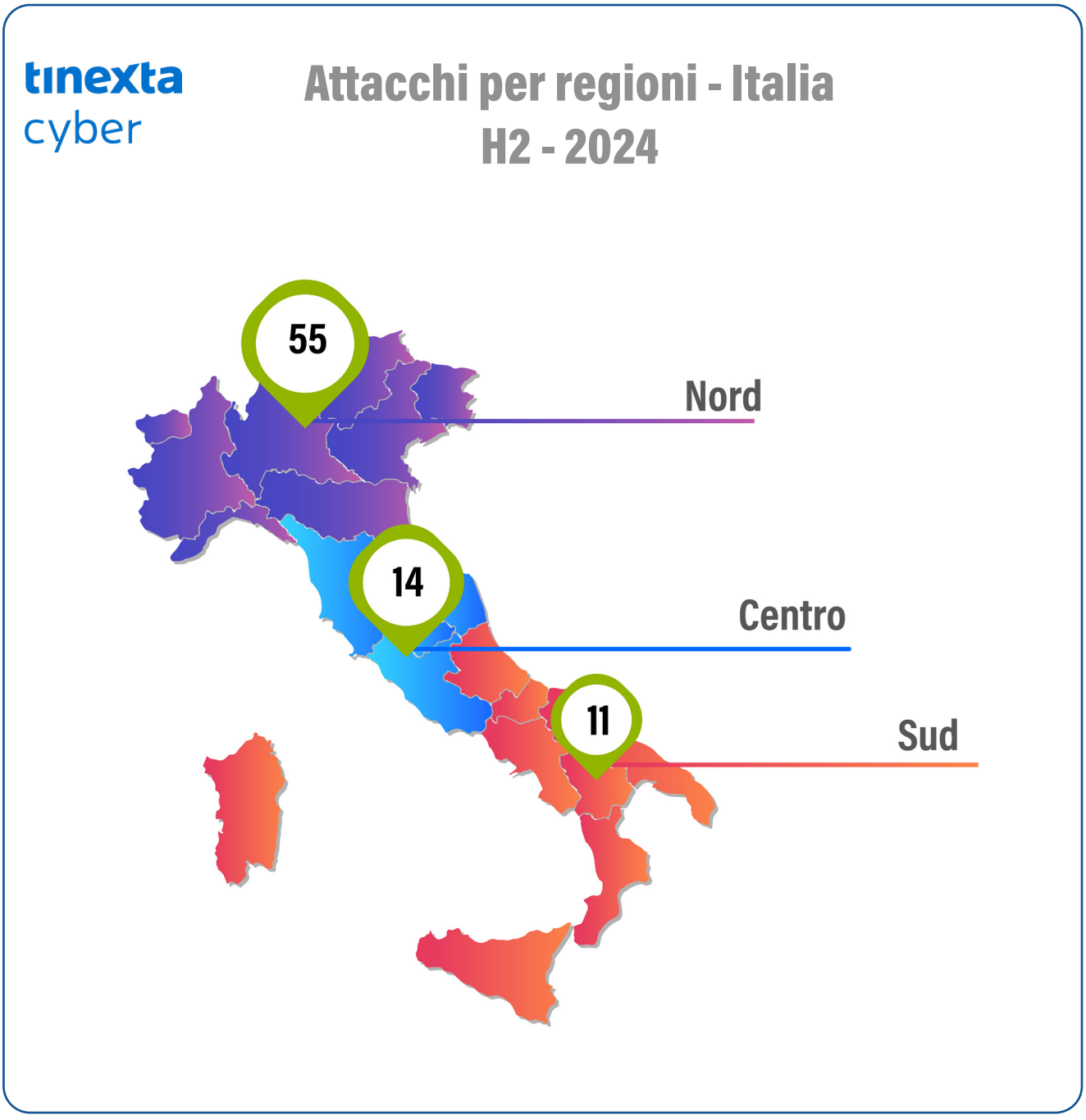
- Un blocco delle attività genera perdite enormi, il che aumenta le probabilità che le vittime paghino il riscatto.
- Le informazioni finanziarie, sanitarie o industriali sono molto appetibili per il mercato nero.
- Dall'uso di sistemi OT obsoleti nella manifattura ai dati sensibili della sanità, ogni settore ha punti deboli sfruttabili dai criminali informatici.

La situazione in Italia: un contesto in evoluzione

L'**Italia**, nonostante un calo del 20,45% nelle minacce nel primo semestre 2024 rispetto al 2023 (da 88 a 70 attacchi), ha visto un'inversione di tendenza nel **secondo semestre**, con un **aumento del 14,29%** (80 attacchi totali) rispetto al primo semestre 2024.



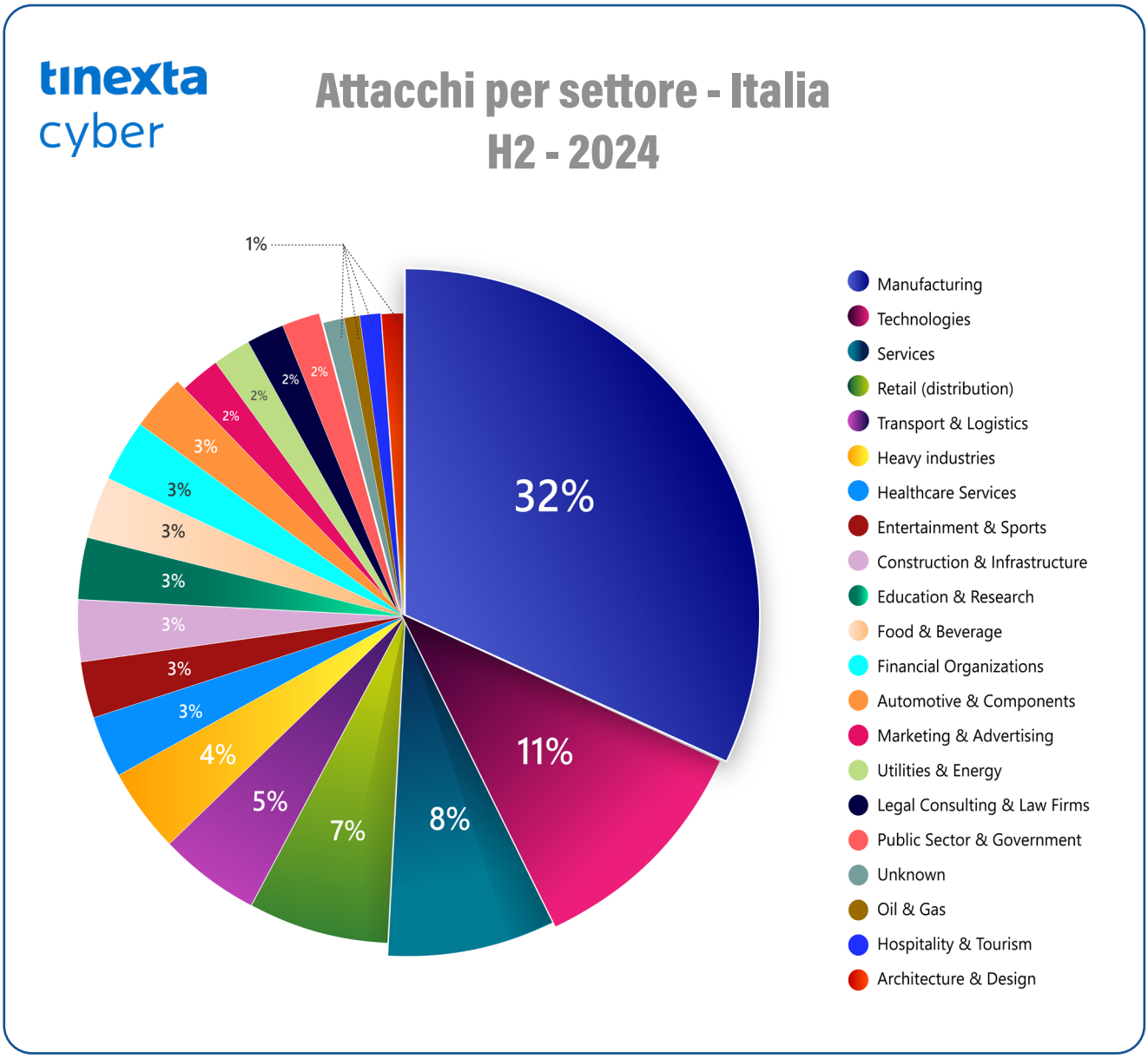
Questa crescita posiziona il Paese al quarto posto nella classifica globale, dopo Stati Uniti, Canada e India, con una distribuzione geografica che vede il Nord Italia assorbire il **55** degli attacchi (42 nel Q4 vs 38 nel Q3). Il Nord, cuore industriale del Paese, è particolarmente esposto a causa della concentrazione di PMI manifatturiere, spesso caratterizzate da infrastrutture IT obsolete e budget limitati per la sicurezza. Il Centro (**14**) e il Sud (**11**) rimangono meno colpiti, ma la tendenza è in crescita, soprattutto in regioni come la Campania e la Sicilia, dove la digitalizzazione accelera ma la consapevolezza rimane bassa.



Settori critici e vulnerabilità italiane

Il settore **manifatturiero** domina la scena con il **32%** degli attacchi, seguito dalle **tecnologie (11%)** e dai **servizi (8%)**.

Questo focus riflette la struttura economica italiana, dove aziende manifatturiere – spesso integrate in catene di fornitura globali – sono vulnerabili a interruzioni che possono paralizzare interi processi produttivi. Il calo dei servizi (dall'11% all'8%) potrebbe essere legato a miglioramenti nelle politiche di sicurezza aziendale, mentre il comparto sanitario (3%) rimane meno esposto rispetto ad altri paesi europei, nonostante alcuni casi isolati di attacchi a ospedali del Nord.

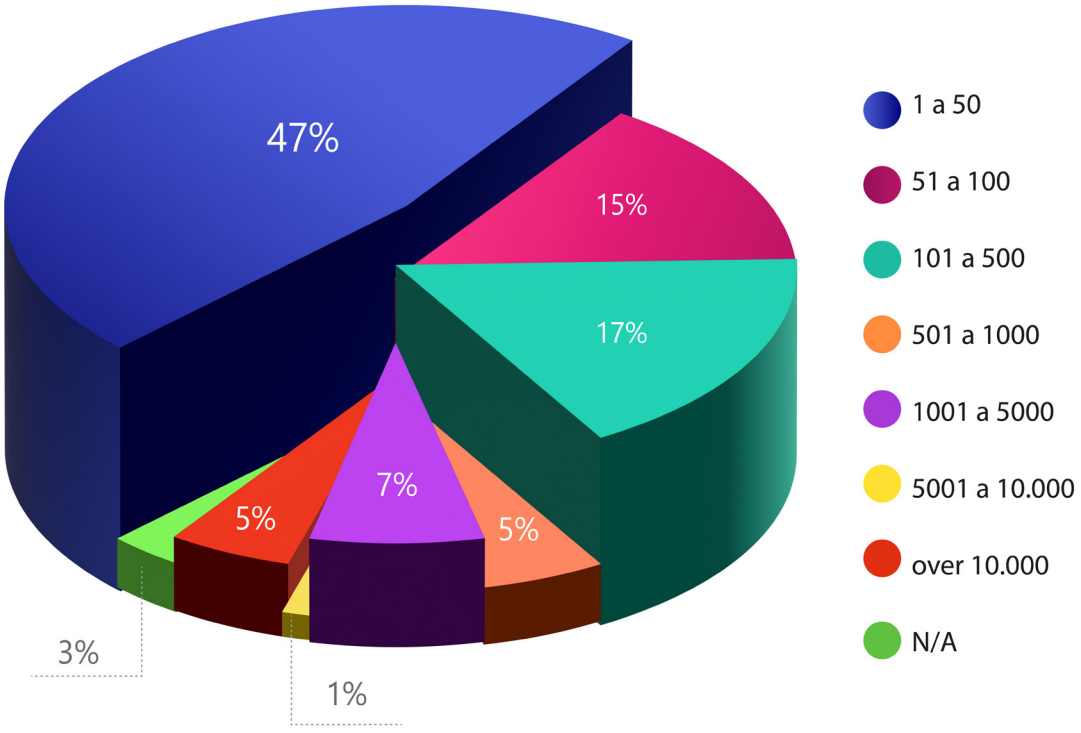


Per dimensione aziendale, il **47%** degli attacchi ha riguardato realtà con 1–50 dipendenti, confermando che le PMI sono il "terreno fertile" per i ransomware.

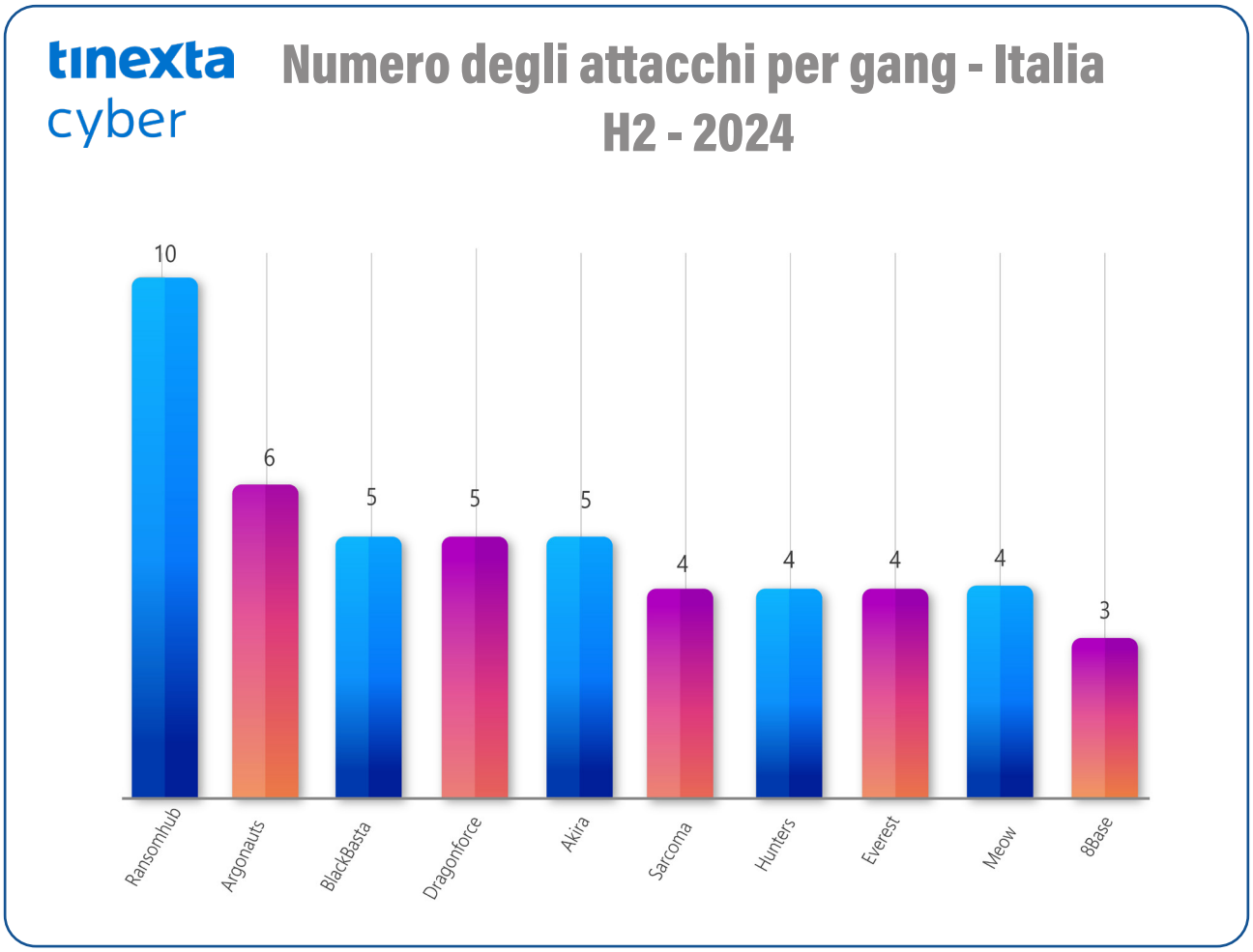
Tuttavia, si nota un incremento significativo (+7%) negli attacchi a imprese con 1.001–5.000 dipendenti, un segnale che i criminali stanno alzando l'asticella per ottenere riscatti più elevati. Anche le aziende con fatturato inferiore a 250 milioni di dollari rappresentano l'83% dei casi, seppur con un lieve calo rispetto all'H1 2024 (-3%). Questo dato sottolinea come le piccole e medie imprese rimangano il bersaglio preferito, ma suggerisce anche un interesse crescente verso realtà più grandi, con fatturati fino a 3 miliardi di dollari (2% degli attacchi).

tinexta cyber

Numero Dipendenti Aziende Colpite Italia - H2 2024



Gang attive e dinamiche criminali in Italia



Il panorama italiano è dominato da **RansomHub**, responsabile del 12,5% degli attacchi (10 casi), seguita da **Argonauts** (6 attacchi) e **BlackBasta** (5).

Nuovi attori come DragonForce hanno quintuplicato la loro attività (da 1 a 5 attacchi), mentre Medusa è scomparsa e 8Base ha ridotto le operazioni del 57% (da 7 a 3).

Tra le gang emergenti, Sarcoma (4 attacchi) e Argonauts si sono affermate rapidamente, sfruttando probabilmente la debolezza di alcune nicchie di mercato. Al contrario, Hunters International, pur presente nella top 10, ha subito un calo globale degli attacchi (-62,62%), riflettendo una possibile ristrutturazione interna o pressioni investigative.

Conclusioni e prospettive per l'Italia

L'Italia si trova a un bivio: da un lato, la crescita degli attacchi nel secondo semestre 2024 sottolinea la necessità urgente di politiche nazionali più incisive; dall'altro, la concentrazione nel Nord e il focus su settori chiave come il manifatturiero richiedono interventi mirati.

Il governo ha recentemente annunciato piani per rafforzare la cybersecurity delle PMI, ma l'implementazione è ancora lenta. Senza investimenti in formazione, condivisione di intelligence tra settore pubblico e privato, e adozione di standard minimi di sicurezza (come la certificazione ISO 27001), il Paese rimarrà un anello debole nella catena globale della cybersecurity. Inoltre, la crescente sofisticazione dei gruppi ransomware – come dimostrato dall'ascesa di RansomHub e Argonauts – impone una risposta altrettanto dinamica, che includa non solo difesa passiva ma anche offensive legali e collaborazione internazionale.

Il ruolo delle istituzioni e delle aziende

Le istituzioni italiane devono accelerare l'attuazione della Direttiva NIS2 e promuovere piattaforme di condivisione delle minacce, come il CERT-Nazionale, per migliorare la resilienza delle aziende. Parallelamente, le imprese devono abbandonare l'approccio reattivo e adottare strategie proattive:

- formazione del personale,
- segmentazione delle reti,
- implementazione di sistemi di backup offline
- monitoraggio continuo delle vulnerabilità.

Solo così sarà possibile contrastare un fenomeno che, nel 2024, ha dimostrato di essere più adattivo e distruttivo che mai.

Se il 2024 ha mostrato un aumento degli attacchi, il 2025 potrebbe portare sfide ancora maggiori. L'avvento dell'intelligenza artificiale generativa, ad esempio, potrebbe essere sfruttato dai criminali per automatizzare la creazione di phishing mirati o l'identificazione di vulnerabilità. In Italia, dove il 47% delle aziende non dispone di un piano di risposta agli incidenti, il rischio è che questa tecnologia amplifichi i danni. È fondamentale, quindi, che il Paese si prepari a un futuro in cui la cybersecurity non sarà più un optional, ma un pilastro della sicurezza nazionale.

CVE Trends

CVE ID	Descrizione	CVSScore
CVE-2024-6409	Vulnerabilità di race condition in OpenSSH (sshd). Un attaccante remoto può sfruttare funzioni non async-signal-safe per eseguire RCE come utente non privilegiato.	7.0
CVE-2024-38206	Un attaccante autenticato può bypassare SSRF in Microsoft Copilot Studio per rubare informazioni sensibili su una rete.	8.5
CVE-2024-23663	Controllo di accesso improprio in Fortinet FortiExtender permette a un attaccante di creare utenti con privilegi elevati tramite richiesta HTTP manipolata.	8.8
CVE-2024-9680	Use-after-free in Animation timelines consente remote code execution. Segnalazioni di exploit in natura. Interessa Firefox, Firefox ESR e Thunderbird.	9.8
CVE-2024-7593	Implementazione errata di autenticazione in Ivanti vTM permette a un attaccante remoto non autenticato di bypassare l'autenticazione del pannello di amministrazione.	9.8
CVE-2024-7589	Gestore di segnali in sshd(8) chiama funzioni non async-signal-safe. Una race condition potrebbe consentire RCE non autenticato come root.	8.1
CVE-2024-20424	Vulnerabilità nell'interfaccia web Cisco Secure FMC consente a un attaccante autenticato di eseguire comandi arbitrari sul sistema operativo come root.	9.9

CVE ID	Summary	CVSScore
CVE-2024-0012	Bypass di autenticazione in Palo Alto Networks PAN-OS consente a un attaccante non autenticato di ottenere privilegi di amministratore PAN-OS.	9.8
CVE-2024-9474	Vulnerabilità di escalation dei privilegi in Palo Alto Networks PAN-OS consente a un amministratore di eseguire azioni sul firewall con privilegi root.	7.2
CVE-2024-11477	Vulnerabilità di Remote Code Execution causata da Integer Underflow nella decompressione Zstandard di 7-Zip. Un attaccante può eseguire codice arbitrario nel contesto del processo corrente.	7.8
CVE-2024-43498	Vulnerabilità di Remote Code Execution in .NET e Visual Studio.	9.8
CVE-2024-10905	IdentityIQ permette accesso HTTP/HTTPS a contenuti statici protetti. Interessa versioni fino a 8.4p2, 8.3p5, 8.2p8 e precedenti.	10
CVE-2024-8785	Nelle versioni di WhatsUp Gold prima del 2024.0.1, un attaccante remoto può modificare valori di registro tramite NmAPI.exe.	9.8
CVE-2024-49138	Vulnerabilità di Elevation of Privilege nel driver Windows Common Log File System.	7.8

Malware

Il Ruolo del MaaS (Malware-as-a-Service) nella Diffusione di Malware

Un fattore comune tra questi tre malware è la loro disponibilità nel modello MaaS (Malware-as-a-Service). Questo approccio ha reso il cybercrimine più accessibile anche a soggetti con competenze tecniche limitate: chiunque può affittare o acquistare versioni di malware come Lumma Stealer, FormBook o AgentTesla su forum del dark web e utilizzare infrastrutture già pronte per la loro distribuzione.

Questa industrializzazione del cybercrimine ha contribuito alla diffusione massiva degli infostealer, con campagne malevole che prendono di mira aziende e utenti in tutto il mondo. Gli attacchi non sono più limitati a specifici settori, ma si estendono a qualsiasi contesto in cui i dati sensibili possano essere monetizzati.

I Malware Più Diffusi: Lumma, FormBook e AgentTesla

Negli ultimi anni, alcuni malware si sono affermati come minacce persistenti nel panorama cybercriminale, con una diffusione capillare e tecniche di attacco sempre più sofisticate. Tra i più rilevanti troviamo Lumma Stealer, FormBook e AgentTesla, tre tipologie di malware che mirano prevalentemente al furto di dati sensibili e credenziali, sfruttando diverse strategie di distribuzione.

- **Lumma Stealer:**

  Lumma Stealer è attualmente uno degli infostealer più diffusi, noto per la sua capacità di sottrarre credenziali di accesso, cookie dei browser, dettagli di carte di credito e portafogli di criptovalute. È spesso distribuito tramite tecniche di social engineering, tra cui commenti malevoli su GitHub, falsi strumenti basati su AI generator e annunci pubblicitari infetti. Questo malware è anche venduto come Malware-as-a-Service (MaaS) nei forum underground, permettendo a cybercriminali meno esperti di utilizzarlo senza dover sviluppare codice proprio.

  Ciò che rende Lumma Stealer particolarmente insidioso è la sua costante evoluzione: gli sviluppatori del malware rilasciano aggiornamenti frequenti per migliorare la sua capacità di elusione dei sistemi di sicurezza. Inoltre, il malware è spesso associato a dropper avanzati, programmi progettati per installare ulteriori minacce sui dispositivi compromessi, aumentando così il danno potenziale.

- **FormBook:**

  FormBook è un altro infostealer che ha mantenuto una posizione dominante tra le minacce informatiche. Questo malware è particolarmente popolare tra i cybercriminali grazie alla sua facilità d'uso e alle sue capacità di evasione, che gli consentono di superare molte protezioni di sicurezza standard.

  FormBook viene distribuito principalmente attraverso campagne di phishing, utilizzando email con allegati infetti, documenti Office con macro malevole o file PDF contenenti exploit. Una volta

installato, il malware raccoglie credenziali di accesso da browser e client email, estrae dati sensibili da moduli online e può persino registrare gli input da tastiera (keylogging).

Uno degli aspetti più critici di FormBook è la sua capacità di persistenza: il malware si nasconde all'interno del sistema e utilizza tecniche avanzate per impedire la sua rimozione, garantendo un accesso prolungato ai dati dell'utente. Inoltre, essendo venduto come malware su abbonamento, viene costantemente aggiornato con nuove funzionalità, aumentando così la sua efficacia nel tempo.

- **AgentTesla:**

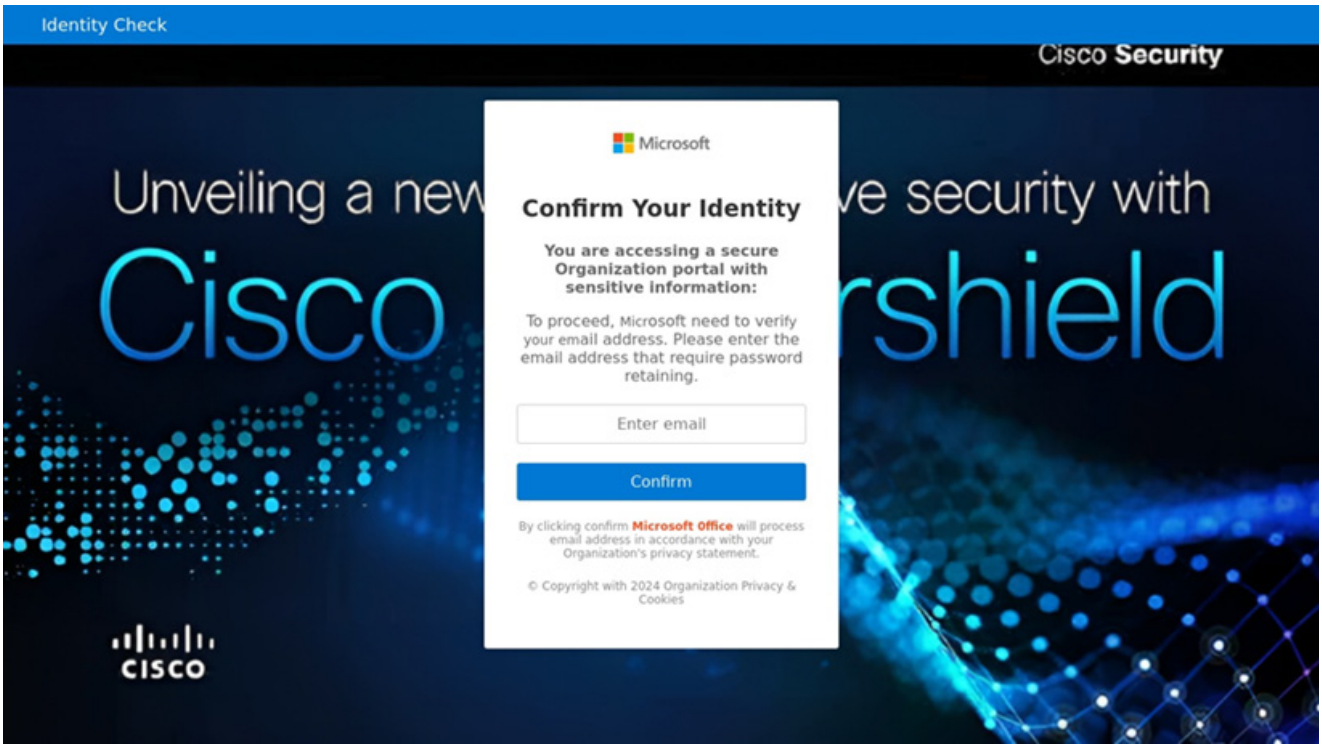
AgentTesla è un Remote Access Trojan (RAT) utilizzato per rubare credenziali, esfiltrare dati aziendali e registrare l'attività della tastiera degli utenti. Questo malware viene spesso veicolato attraverso allegati email dannosi, mascherati da fatture, notifiche di spedizione o documenti aziendali urgenti.

Una delle caratteristiche distintive di AgentTesla è la sua capacità di operare come keylogger e stealer contemporaneamente, catturando informazioni dai browser, client di posta elettronica e software FTP utilizzati dalla vittima. Oltre a ciò, il malware può anche prendere screenshot dello schermo della vittima e inviare periodicamente le informazioni raccolte ai server controllati dagli attaccanti.

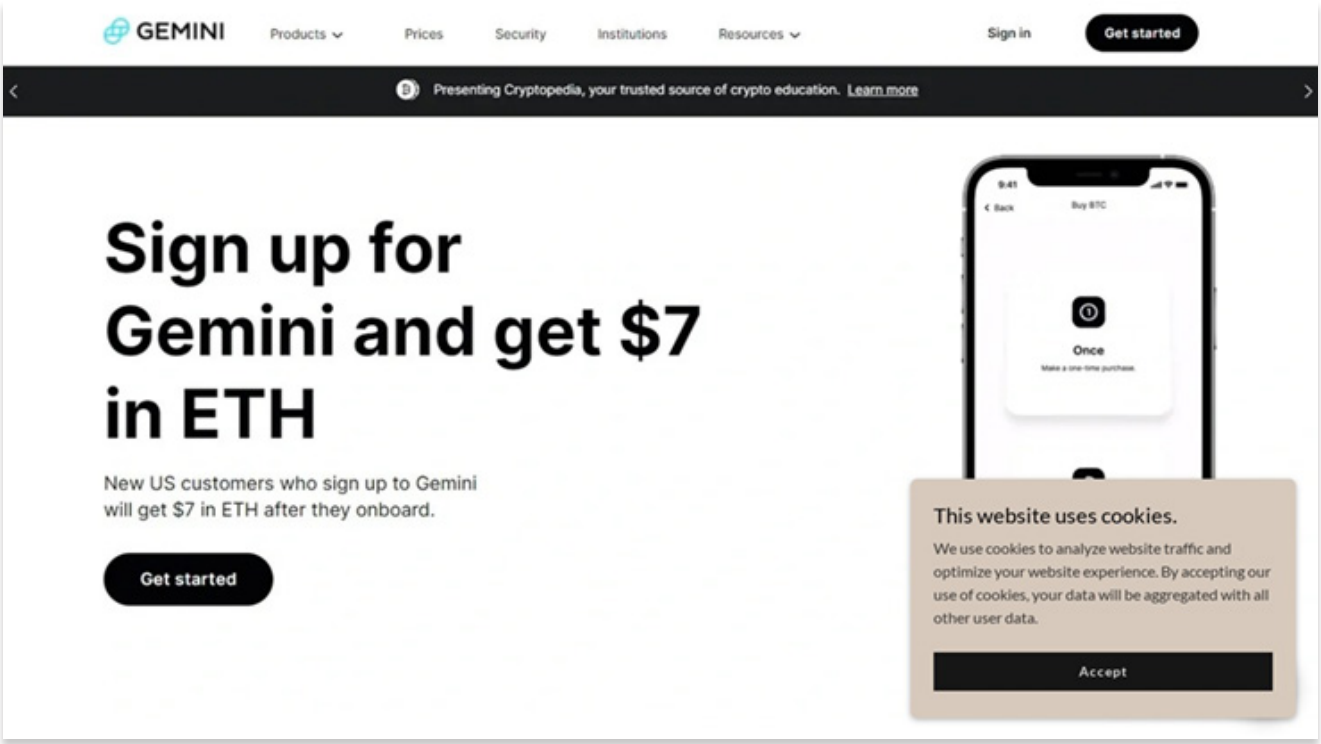
Ciò che rende AgentTesla una minaccia persistente è la sua modularità: gli sviluppatori del malware continuano ad aggiornarlo per migliorare la sua capacità di aggirare le protezioni antivirus e firewall. Inoltre, grazie a tecniche di offuscamento avanzate, riesce a nascondersi nei sistemi compromessi per lunghi periodi senza essere rilevato.

Phishing

Nel **secondo semestre del 2024**, gli attacchi di phishing hanno continuato a colpire una vasta gamma di bersagli, con una crescente preferenza per obiettivi di alto valore economico o strategico. Tra i settori più esposti, il comparto tecnologico e i servizi cloud si sono rivelati particolarmente vulnerabili. La crescente dipendenza delle imprese da queste infrastrutture ha creato un ecosistema fragile, in cui gli attaccanti hanno sfruttato falle nei sistemi di gestione delle identità e configurazioni errate dei server per compromettere intere reti aziendali.



Parallelamente, anche il mondo delle criptovalute è diventato un obiettivo primario, complice la crescente popolarità del settore e le ingenti somme di denaro in circolazione. Tra le tecniche più utilizzate spiccano l'address poisoning, che induce le vittime a trasferire fondi a indirizzi falsificati, e le campagne di falsi airdrop, con giveaway fraudolenti finalizzati a sottrarre le credenziali dei wallet digitali.



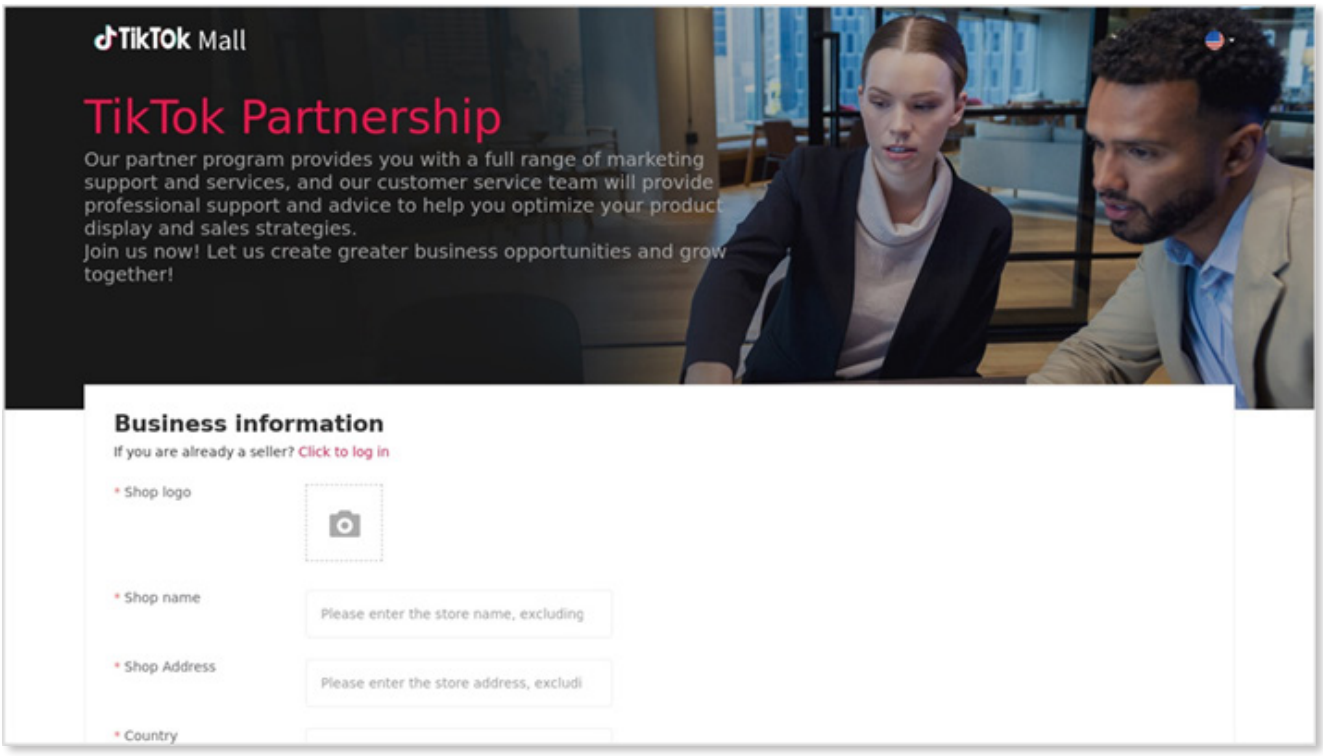
Dalle elezioni presidenziali USA alle campagne di shopping natalizio, passando per attacchi alle infrastrutture di telecomunicazione e ai social media, il phishing si è confermato uno strumento estremamente versatile e pericoloso.

Gli hacker hanno affinato le loro tecniche, integrando l'intelligenza artificiale (IA) per generare e-mail sempre più realistiche e convincenti. Grazie all'IA, possono simulare in modo preciso il linguaggio e lo stile di comunicazione di aziende e individui, rendendo gli attacchi più difficili da individuare.

Un ulteriore aspetto cruciale della diffusione dell'IA è la riduzione delle barriere tecniche, che ha reso l'organizzazione di campagne di phishing accessibile anche a chi ha competenze informatiche limitate. Sebbene i principali vendor abbiano implementato restrizioni per impedire l'uso delle loro tecnologie in attività malevole, tali misure sono spesso aggirabili tramite tecniche di prompt engineering avanzato e l'utilizzo di modelli LLM eseguiti localmente.

Un altro fattore chiave nella crescita del phishing è stato l'uso massiccio dei social network come vettore di attacco. Facebook e TikTok sono state tra le piattaforme più sfruttate per diffondere campagne fraudolente, spesso sotto forma di finto supporto clienti, messaggi diretti o annunci pubblicitari. Facebook, con una base utenti mediamente più adulta e con maggiore disponibilità economica, è un bersaglio ideale per gli attaccanti, che sfruttano la minore consapevolezza informatica di questa fascia d'età per orchestrare truffe finanziarie o rubare credenziali.

TikTok, invece, è diventato un vettore sempre più efficace grazie alla sua crescente popolarità e continua evoluzione normativa. La decisione di vietare TikTok negli Stati Uniti, seguita dal successivo ripristino della piattaforma, ha offerto ai threat actor l'opportunità di sfruttare la bolla mediatica per lanciare campagne di phishing mirate. La costante introduzione di nuove funzionalità rende più credibili comunicazioni di presunto supporto tecnico o richieste di verifica dell'account, aumentando il rischio di attacchi mirati.



Gli attaccanti stanno inoltre sfruttando piattaforme cloud affidabili come GitHub, Microsoft OneDrive e Google Drive per ospitare landing page, che reindirizzano le vittime verso domini fraudolenti con login contraffatti. Di recente, questa pratica è stata osservata anche attraverso Zoom Docs, il nuovo servizio di Zoom rilasciato ufficialmente ad agosto 2024. Il suo utilizzo diffuso in ambito enterprise lo rende un vettore particolarmente credibile per campagne di phishing mirate. Approfittando dell'implicita fiducia che gli utenti ripongono in questi servizi e della reputazione di cui gode il servizio cloud, riescono a eludere i filtri di sicurezza aziendali, rendendo questi attacchi particolarmente insidiosi.

Per questo motivo, la consapevolezza degli utenti rimane la prima linea di difesa. Investire in programmi di cybersecurity awareness è essenziale per insegnare a riconoscere i segnali d'allarme nelle email, come un'eccessiva urgenza, errori grammaticali o richieste insolite di login e download. La protezione contro il phishing non può più basarsi solo su soluzioni tecnologiche: serve un approccio integrato che combini educazione, tecnologia e vigilanza continua.

Trend Futuri

Abuso dell'IA e Data Breach attraverso Modelli Open

L'uso improprio dell'intelligenza artificiale sta aumentando con l'accesso diffuso a modelli open-source, rendendo più facili attacchi come data breach mirati. I cybercriminali possono sfruttare queste IA per analizzare database, individuare vulnerabilità e automatizzare attacchi su larga scala, mettendo a rischio aziende e utenti finali.

Ransomware AI: Bot che Negoziano con le Vittime

Gli attacchi ransomware stanno evolvendo grazie all'IA, con bot avanzati capaci di negoziare direttamente con le vittime per il pagamento del riscatto. Questi bot analizzano il comportamento delle aziende colpite, adattando le richieste economiche e rendendo le operazioni di estorsione più efficienti e convincenti.

Malware Polimorfico con IA: Virus Vivente

I malware polimorfici alimentati dall'IA stanno diventando una delle minacce più pericolose. Questi software malevoli si adattano costantemente ai sistemi di rilevamento, modificando codice e comportamento in tempo reale. Questi malware possono rimanere dormienti o evolversi per sfuggire alle misure di sicurezza tradizionali.

Crescita delle Regolamentazioni: DORA e NIS2

L'aumento delle minacce informatiche ha portato a nuove normative come DORA (Digital Operational Resilience Act) e NIS2 (Network and Information Security Directive 2), che mirano a rafforzare la resilienza digitale delle infrastrutture critiche. Queste regolamentazioni impongono standard di sicurezza più rigidi per aziende e istituzioni, aumentando le sanzioni per la mancata conformità.

Attacchi alla Supply Chain attraverso la Manipolazione Open-Source

La dipendenza da software open-source ha reso la supply chain IT un bersaglio prioritario. I cybercriminali manipolano pacchetti open-source per introdurre backdoor o malware che, una volta integrati in software di terze parti, compromettono intere reti aziendali. Questo trend

mette in pericolo anche le aziende più sicure, poiché l'attacco avviene indirettamente attraverso fornitori fidati.

Deepfake: Digital Twin e Doppelgänger per Frodi Avanzate

Le tecnologie deepfake stanno diventando strumenti sofisticati per frodi e attacchi mirati. Con la creazione di "digital twins" e "doppelgänger" digitali, i criminali possono impersonare dirigenti aziendali o celebrità, orchestrando truffe convincenti, dal furto di identità ai falsi ordini di pagamento.

Hacking e Truffe nel Metaverso e VR/AR

Con la crescita del metaverso e delle tecnologie di realtà aumentata/virtuale, emergono nuovi vettori di attacco. Gli hacker possono manipolare ambienti virtuali, intercettare dati biometrici o eseguire truffe sfruttando avatar fasulli per ingannare gli utenti. Queste vulnerabilità rappresentano un serio rischio per il futuro della sicurezza digitale in ambienti immersivi.

La Crescita degli Infostealer: Il Caso di Lumma Stealer

Lumma Stealer è emerso come una minaccia rilevante nel panorama dei malware, distinguendosi per la sua capacità di sottrarre una vasta gamma di informazioni, tra cui credenziali di accesso, cookie del browser, dettagli di carte di credito e cronologia di navigazione. Questo malware è noto per sfruttare piattaforme legittime come GitHub per diffondersi, aumentando così la sua portata e l'efficacia degli attacchi.

Una delle tecniche utilizzate da Lumma Stealer consiste nell'inserire commenti malevoli all'interno di discussioni su progetti GitHub. Questi commenti spesso contengono link a file apparentemente utili, ma che in realtà scaricano ed eseguono il malware sul sistema della vittima. Questo metodo sfrutta la fiducia degli sviluppatori nella comunità open-source, rendendo più probabile l'infezione.

Un'altra strategia adottata dai distributori di Lumma Stealer è la creazione di falsi strumenti di generazione video basati sull'intelligenza artificiale. Ad esempio, nell'ottobre 2024, sono stati segnalati casi in cui finti generatori di video AI per Windows e macOS erano in realtà veicoli per l'installazione di Lumma Stealer sui dispositivi degli utenti. Questo approccio sfrutta l'interesse crescente verso le tecnologie AI, attirando utenti desiderosi di sperimentare nuovi strumenti.

L'Incremento degli Attacchi su macOS: Il Caso di AMOS

Tradizionalmente considerato più sicuro rispetto ad altri sistemi operativi, macOS ha visto un aumento significativo degli attacchi malware. Un esempio è AMOS (Atomic macOS Stealer), un malware-as-a-service progettato specificamente per colpire utenti macOS. Gli affiliati che distribuiscono AMOS utilizzano diverse tecniche, tra cui il Google Ads poisoning e la creazione di falsi repository su GitHub, per ingannare gli utenti e indurli a scaricare software compromesso. Una volta installato, AMOS esfiltra dati sensibili come cookie, password e dettagli di carte di credito, che vengono poi venduti su forum del dark web.

Sfruttamento di Eventi di Attualità per la Diffusione di Malware

I cybercriminali spesso capitalizzano su eventi di grande risonanza mediatica per aumentare l'efficacia delle loro campagne malevole. Temi come il gaming, le criptovalute, l'intelligenza artificiale e manifestazioni sportive globali come le Olimpiadi vengono utilizzati come esca per attirare le vittime. Ad esempio, durante periodi di alta attenzione verso le criptovalute, sono state osservate campagne di phishing che promettevano guadagni facili attraverso investimenti in nuove monete digitali, ma che in realtà distribuivano malware progettati per sottrarre portafogli digitali e credenziali di accesso.

tinexta cyber

Analysis by:

Riccardo Michetti
Luigi Martire
Riccardo D'Ambrosio
Martina Fonzo
Veronica Chierzi
Dardan Baljaj

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

Milano
+39 02 6666 1442
www.tinextacyber.com
info@tinextacyber.com
Vetra Building, Via Fernanda Wittgens, 2, MI